MISTRAL: A game-theoretical model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries

Luca Talarico[a], Genserik Reniers[b,c], Kenneth Sörensen[a], Johan Springael[a]

[a] *Faculty of Applied Economics, Research Groups ANT/OR, University of Antwerp, Prinsstraat 13, 2000 Antwerp, Belgium*
[b] *Center for Corporate Sustainability (CEDON), HUB, KULeuven, Stormstraat 2, 1000 Brussels, Belgium*
[c] *Safety Science Group, TU Delft, Jaffalaan 5, 2628 BX Delft, The Netherlands*

Abstract

In this paper we present a multi-modal security-transportation model to allocate security resources within a chemical supply chain which is characterized by the use of different transport modes, each having their own security features. We consider security-related risks so as to take measures against terrorist acts which could target critical transportation systems. The idea of addressing security-related issues, by supporting decisions for preventing or mitigating intentional acts on transportation infrastructure, has gained attention in academic research only recently. The decision model presented in this paper is based on game theory and it can be employed to organize intelligence capabilities aimed at securing chemical supply chains. It enables detection and warning against impending attacks on transportation infrastructures and the subsequent adoption of security countermeasures. This is of extreme importance for preventing terrorist attacks and for avoiding (possibly huge) human and economic losses. In our work we also provide data sources and numerical simulations by applying the proposed model to a illustrative multi-modal chemical supply chain.

Keywords: Multi-modal transportation, Security, Risk analysis, Game-theory, Multi-attribute utility

1. Introduction

In Europe and in the United States, huge amounts of hazardous materials (hazmat) are continuously transported. Daily shipments of dangerous goods are in fact critical to the economies of Europe, U.S., and the rest of the world. However, these transportation activities involve various types of security risks.

Email address: Corresponding author: luca.talarico@uantwerpen.be (Luca Talarico)

In case of (even minor) incidents, dangerous freights would strongly attract the attention of the general public, policy makers and industrialists. It is thus essential, as much for the responsible government as for the private authorities, to efficiently secure these hazardous transports. Take the complex chemical supply chain as an example, we could consider it as a single, complete system starting from the raw materials supplier, through the manufacturing and distribution process, to the final end-use customer, and any residuals management, including the transportation network in between [1]. Since a lot of stakeholders are involved, it is not easy to adequately and efficiently secure a chemical transportation supply chain. Moreover, it should be noted that the threats of intentional attacks on the chemical supply chain substantially differs from the one of unintentional incidents. While the *unintentional accident* likelihood depends on (relatively) well-known parameters such as maintenance of infrastructure, speed characteristics and the presence of junctions, the *intentional accident* likelihood relates to much less known factors such as vulnerabilities, consequences, and intentions.

One of the key factors of the chemical supply chain is multi modality; i.e., the use of different transport modes, each having their own characteristics with respect to economic and environmental parameters, as well as characterized with safety and security mode-specific features (see e.g. [2]). Multi-modal transportation is very much prevalent in the chemical industry, using road, railway, barges, ships, and pipelines to transport goods. The majority of transportation firms are specialized in one single transportation mode; they rarely operate combining several modi on their own. For example a shipper company that is specialized in maritime transportation, has to rely on a different carrier to transport, by ground vehicles, a product to a final customer. Nonetheless, by transporting chemical products employing different modes, (e.g. moving goods from road onto rail, ship or pipeline or vice versa, for security considerations), the chemical industry and its logistic service providers could greatly improve their security scores.

Hence, the security resource allocation problem exists on both intra- and inter-modal levels. On an intra-modal dimension, the authorities or the companies responsible for the transport have to decide on which transportation routes (belonging to the same mode, that is road, rail-road, inland waterways or pipeline) available between point A and point B (A and B being e.g. a company, a city, or a storage park) security measures have to be taken. This decision regarding security resources allocations should take into account all critical unimodal transportation routes between A and B and it should be repeated for every dangerous freight the authorities or the companies wish to investigate. On an inter-modal dimension, the different available modi for transporting a certain hazardous cargo between A and B should be investigated and security resources need to be allocated between the different modi, which forms an extra complexity to the uni-modal security resources allocation problem. Actually, multi-modal planning is more difficult than uni-modal planning, both on an operational (i.e., planning of individual shipments), and on a tactical/strategic level (i.e., planning of flows of goods through the network). Therefore, an even

stronger need for support by a transportation security risk model is present in the multi-modal case.

Three research lines are present in scientific literature regarding the development of safety decision support software for transports of dangerous freights: (i) safety-related risk assessment software packages [3–9]; (ii) route selection and vehicle scheduling software packages [10–14]; and (iii) hazardous materials network design software [15–19]. Note that these software packages dealing with *safety*-related transport problems are designed to guide uni-modal decisions. Among these useful models there are probabilistic tools, GIS-based tools, tools ensuring an equitable distribution of risk, tools based on the iterative application of minimum path algorithms, tools based on the generation of minimum paths, tools based on multi-objective algorithms, bi-levels programming tools (taking into account two distinct decision-makers: the government and transport companies), and tools based on heuristic algorithms.

However, the idea of developing such software packages addressing security-related issues and specifically aiming them at supporting decisions for preventing or mitigating intentional designed malicious acts on transportation infrastructure, has only very recently gained attention in the academic world. We are aware that various conceptualisations and software packages (GIS-based or not) for dangerous freight risk assessments capturing one or several of the transport modes, have been elaborated and are explained in literature. However, these software applications are aimed at safety related (non-intentional) risks and they could not be used for taking measures against intentional (terrorist) acts. In fact, to our knowledge, at present there is no model of dangerous substances transportation available to governmental or industrial decision makers building on multi-attribute utility functions and providing recommendations about where to optimally allocate security measures and resources in a multi-modal chemical transportation network (e.g. in the United States or in Europe). This paper elaborates such a model using game theory.

2. Game theory used in security problems

Since the terrorist attacks on 11 September 2001, game theory has been increasingly employed as a mathematical tool to deal with security decisions facing with adaptive adversaries. In particular, recent literature includes [20–25] and [26]. The reader is referred to [27] and [28] for an extensive survey. More specifically, gaining insights into the nature of optimal defensive investments yielding the best trade-off between investment costs and critical infrastructure security was also already subject of an important amount of scientific research (see e.g. [29–41]).

However, to date, no concrete attention has been paid to the multi-modal transportation security resources allocation decision problem. This is thus a research subject deserving much more attention from the academia. In fact, the cost on the entire supply chain of a weapon of mass destruction shipped via containers is estimated to be $1 trillion, whereas the September 11 attacks on

the two World Trade Center buildings only costed some $83 billion direct and indirect costs [42].

Organizing intelligence capabilities to detect and to warn of impending attacks on transportation infrastructure and subsequently allocating and taking security countermeasures is thus one of extreme importance for preventing terrorist attacks and for avoiding huge human and economic losses.

We agree with Cox [43] that game theory and risk analysis are mutually reinforcing in order to obtain effective risk management recommendations for allocating security resources. In case of our multi-modal transportation problem, we choose to focus on the development of an attacker-defender model based on game theory. We consider a dynamic game with incomplete information in which the defender chooses how to allocate the security resources (e.g. on which transport routes, on which modes), and then an attacker chooses which target to attack (e.g. which route, which mode) according to a multi-attribute utility function. A model focusing on multi-modal transportations of hazardous substances should make the decision process of taking security countermeasures allocations in a complex transportation network more objective and (subsequently) more justified. The internal parameters of the model can be tuned by the decision maker in a really easy way in order to cope with realistic and customized scenarios.

In the remainder of the paper we will refer to a *strategic game* as a model in which a set of decision makers interact with each others. In recognition of the interaction, we will use the term *players* to identify the decision makers.

The aims of this paper are to (i) include a ranking of transportation routes and modes where to allocate security countermeasures based on certain assumptions; and (ii) provide this ranking considering both inter- and intra-modal transports of hazardous goods.The remainder of this paper is organized as follows: Section 3 sets up a one-period multi-modal security-transportation model. Section 4 provides data sources and numerical simulation. Section 5 elaborates on the description of the solution approach. Experimental tests are also presented. Section 6 concludes this paper and provides some future research directions.

3. A multi-modal security-transportation model

In this paragraph we describe a **M**ult**I**-modal **S**ecurity-**TRA**nsportation mode**L**, that we named $\mathcal{MISTRAL}$ for short, that can be concretely adopted to increase the security of chemical transportation networks. Supply chains used to transport hazardous materials represent a viable target for terrorist groups mainly due to the following factors:

- the physical and chemical properties of the transported material may cause a malicious release which could potentially engender public injuries to a neighbouring population and/or environmental damages;
- the critical importance of the products may determine the disruption of operations of the whole industry along the supply chain.

In general terrorists pick up their targets (e.g. critical infrastructures) for strategic reasons in order to maximize the direct and indirect consequences of the attack [44]. The transported material and its operating conditions (e.g. pressure, temperature, density, volume) are both crucial to determine the criticality of the supply chain. In fact the possible scenarios (e.g. explosions, toxic cloud migrations, thermal radiation effects, toxic releases), that can arise after an attack, influence the level of criticality of a certain supply chain. For this reason, by including other transportation modes which are commonly adopted to transport non-hazardous materials, the $\mathcal{MISTRAL}$ model could be generalized to other supply chains that might be a potential target for terrorists-attackers.

In our study, we focus on four real and tangible transportation modes which are commonly encountered within chemical supply chain: inland waterways ($i = 1$), road transport ($i = 2$), railway ($i = 3$), and pipeline ($i = 4$). As mentioned before, it should be noted that by enlarging the set of available transportation modes the $\mathcal{MISTRAL}$ model could be generalized and extended to other supply chains which are used for non chemical products.

We consider there are r_i routes for each mode i. Therefore, there are altogether $r_1 + r_2 + r_3 + r_4$ routes in the system. For route j in mode i, we let the government's defence level be d_{ij} and let the terrorist's attack level be A_{ij}, for $i = 1, \ldots, 4$ and $j = 1, \ldots, r_i$. The attack (defence) level quantifies the amount of attack (defence) resources such as materials, human resources, technologies, equipment, instrument, expertise, industrial capability and capacity employed by an attacker (defender) to perform a specific action. The probability of damage conditional on an attack happening on each route is a function of d_{ij} and A_{ij}. In particular, we apply the common ratio form contest success function [45], that is:

$$P_{ij}(A_{ij}, d_{ij}) = \frac{A_{ij}}{A_{ij} + \beta_i \cdot d_{ij}} \tag{1}$$

where β_i is the relative defence/attack effectiveness ratio for mode i. We assume that $\beta_1 > \beta_2 > \beta_3 > \beta_4$ (i.e., the inland waterways transports are easiest to defend while pipeline transports are most difficult to defend). It should be noted that the values of βi can be set by the decision maker depending on the specific characteristics of transportation modes i which characterize the supply chain that is considered. The choice made in this paper does not affect the applicability of the model to other supply chain systems where the peculiarities of the transportation modes require a different relationship between the defence/attack effectiveness ratios. Note that we have $\partial P_{ij}/\partial d_{ij} \leq 0$ and $\partial P_{ij}/\partial A_{ij} \geq 0$. We define $P_{ij}(0, d_{ij}) = 0 \; \forall \, d_{ij}$.

In real-life transportation networks, transport modes may present a different topology, with parallel and serial structures, as shown in Figure 1. In this paper, we assume that road ($i = 2$) and pipeline ($i = 4$) have a parallel structure, while

inland waterways ($i = 1$) and railway ($i = 3$) have a serial structure[1].

Assuming performance independence among routes $j = 1, \ldots, r_i$ within a mode i, the vulnerability of mode i, Q_i is calculated as:

$$Q_i(A_i, d_i) = \begin{cases} \prod_{j=1}^{r_i} P_{ij}(A_{ij}, d_{ij}), & \text{if } i = 2, 4 \text{ for parallel structures} \\ 1 - \prod_{j=1}^{r_i} [1 - P_{ij}(A_{ij}, d_{ij})], & \text{if } i = 1, 3 \text{ for serial structures} \end{cases} \tag{2}$$

where $A_i = (A_{i1}, \ldots, A_{ir_i})$ and $d_i = (d_{i1}, \ldots, d_{ir_i})$. Referring to the valuation of route i, we named v_i the conditional expected loss due to a successful attack. We consider two types of losses (direct and indirect) financial loss f_i and human loss h_i) and use the following multi-attribute utility function:

$$v_i = f_i + c \cdot h_i \tag{3}$$

Direct financial losses represents the material damages to e.g. infrastructures, equipments, installations directly induced by an attack, while the indirect financial losses are related to the indirect consequences of the terrorist actions. These latter include also the psychological effects of the attacks on people. In principle also the fear engendered by the terrorists as a direct consequences of an attack may have an impact on a nation's economy and may be quantified in different ways. In particular, the financial impacts on both the transportation and tourism sectors can be estimated as well as it would be possible to quantify the losses in the financial markets and the reduction of foreign direct investment in a country. For more details about how to quantify the consequences of a terrorist attack the reader is referred to[47–49].

In Formula (3) c represents a factor translating human loss into financial terms. Furthermore, we assume that $f_2 < f_4 < f_1 < f_3$ and $h_1 < h_4 < h_2 < h_3$; in other words, road transportation and inland waterways would lead to the lowest possible financial and human losses respectively, and railway would lead to the highest financial and human losses. These are just some assumptions that we made without loss of generality which can be easily changed by the user of the $\mathcal{MISTRAL}$ model to fulfil the requirements of a specific chemical supply chain.

We assume that the government desires to maximize the total expected averted losses, subtracting the total defence costs, while the terrorist wants to maximize the total expected damage, subtracting the total attack costs. In other words, government and terrorist maximize their utilities $u(A, d)$ and $U(A, d)$ respectively as follows:

[1] We acknowledge that this assumption on system structure depends on the scope of the security study, but we believe generally these assumptions are reasonable [46].

$$\max_{d} u(A,d) = \sum_{i=1}^{4}\{v_i \cdot [1 - Q_i(A_i,d_i)] - b \cdot \sum_{j=1}^{n_i} d_{ij}\} \tag{4}$$

$$\max_{A} U(A,d) = \sum_{i=1}^{4}[v_i \cdot Q_i(A_i,d_i) - B \cdot \sum_{j=1}^{n_i} A_{ij}] \tag{5}$$

In Formulae (4)-(5) b and B are the costs of resources unit associated to the adoption of a specific defence of attack strategy respectively. To mention some examples, the *Joint Improvised Explosive Device Defeat Organization*, a Pentagon organization, estimates the costs of resources unit employed by terrorists to carry on a specific terrorist action. In particular a cost of $400 is estimated for an attack made by using a remote-controlled bomb, $1,200 for a suicide bombing vest, while the cost for a suicide car bomb can vary between $13,000 and $20,000 depending on the car that is employed. $A = (A_1 \ldots, A_4)$ and $d = (d_1, \ldots, d_4)$ represent a specific set of possible actions to be adopted by the attacker and the government respectively. In particular these actions are addressed to a specific transportation mode (e.g. $A_i = (A_{i1}, \ldots, A_{ir_i})$ or $d_i = (d_{i1}, \ldots, d_{ir_i})$) each containing j routes. In the remainder of the paper we will refer to A and d with the term *strategies* to denote a specific attack (for A) and defence (for d) actions. The quality of each strategy is measured by using the *utility functions*, mentioned before, which are able to capture and quantify the players' preferences. The main assumptions employed inside the MISTRAL model are summarized in Table I.

It should be noted that in the strategic game the players' payoffs have only a ordinal significance. For example, if a player has three available (attack or defence) strategies named a, b, and c for which the resulting payoff is respectively 1, 2, and 10, the only conclusion that it is possible to draw is that the player prefers c to b and b to a. In other words the values associated to the payoff in themselves do not imply that the player's preference between c and b is stronger than his preference between a and b [50].

Below we consider two possible sequences of move: simultaneous-move and sequential move (where the defender is the first mover). Both sequences have been studied in literature [51–53]. If the defence is public information and terrorists know the defence allocation before making the attacking decisions, a sequential-move model should be used. Otherwise, if both players make decisions at the same time, or at least they do not know the other player's choice at the time that they make their own decisions, a simultaneous-move model should be used.

Definition 1. *We call a pair* (A^*, d^*) *an equilibrium for a simultaneous-move* MISTRAL *game if and only if* $A^* = \arg\max_{A} U(A, d^*)$ *and* $d^* = \arg\max_{d} u(A^*, d)$.

Definition 2. *We call a pair* (A^*, d^*) *an equilibrium for a sequential-move* MISTRAL *game (where the government is the first mover) if and only if*

$A^* = \hat{A}^*$ *and* $d^* = \arg\max_d u(\hat{A}^*, d)$*, where* $\hat{A}^* = \arg\max_A U(A, d)$ *is the best response function.*

4. Data sources and numerical examples

In order to test the $\mathcal{MISTRAL}$ model described before, we present an illustrative system of a chemical supply chain which is represented in Figure 2. In our simplified, but realistic, transportation system we considered three different transportation modes: inland waterways ($i = 1$), road transport ($i = 2$) and railway ($i = 3$). Additionally, we suppose that 2 routes are available for transportation mode $i = 2$. Therefore there are 4 routes in the system. These routes can be combined together to generate two alternative paths to reach the destination node D starting from the origin node O passing through the intermediate nodes m and n. The first path is made by the following transportation modes: inland waterway, road 1 and train. The second path is composed by inland waterway, road 2 and train. In this way it is possible to model a realistic chemical supply chain in which hazmat materials are transported from a production site O to an harbour m by a container ship through an inland waterway, then from the harbour the chemical products are transported by trucks to the closer rail loading station m from which the goods are transported by train directly to the warehouse of raw materials of a chemical company in D.

We suppose that $\beta_1 = 75\%$, $\beta_2 = 60\%$ and $\beta_3 = 45\%$. The value of c is set equal to 200 (reasonable values of c used to transform a human loss into economic values are in the range $1 - 10 \times 10^6$€). Without loss of generality, we suppose that the unit costs for defence are ten times higher than the unit costs for attacks ($b = 10 \cdot B$). This assumption reflects realistic situations in which the government investments in defence strategies are much higher than attackers' investments for terrorist attacks. Therefore in our numerical example we set $b = 100$ and $B = 10$. The values associated to f_i and h_i for each transportation mode i are summarized in Table II.

In our example we suppose that the government's defence level d_{ij} can have a 3-point scale: 1, 2 or 3 (low, medium, or high), depending of the level of investments to secure and to protect route j contained in transportation mode i. The same values can be used to measure the attack levels A_{ij} for all routes j in transportation mode i. This assumption is rather plausible, in fact in the United States a scale based on colors is used to measure the terrorist threats [54]. This scale, also known under the name of "terror alert level", is based on a scale of 5 colors (green, blue, yellow, orange, red) measuring an increasing risk of terrorist attacks (low, general, significant, high, severe). Each level (e.g. red code for severe risk of terrorist attacks) triggers specific actions by the government affecting thus the security level of public facilities. In other words the government adapts its defensive strategies to the possible terrorist threats. A similar scale is currently adopted in Europe in particular in the UK to give to the government a broad indication of the likelihood of a terrorist attack. Five different threat levels (low, moderate, substantial, severe and critical) are based

on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities. Moreover these levels inform decisions about the levels of security needed to protect critical national infrastructures [55].

5. Solution approach

In principle, in a $\mathcal{MISTRAL}$ game, the players' interests are diametrically opposed. The aim of the attacker is to destroy the chemical supply chain while the government is committed to secure it. Moreover if the attacker adopts a successful attack, which determines high financial and human damages, the consequences of the attack are paid by the government whose objective is to secure a given infrastructure, by investing in its protection.

Strategic situations which involve players with completely opposite interests are known in literature as *strictly competitive games*. A two players strictly competitive game is a two players game in which for every two strategies s and $\hat{s}$ the following property holds, where u_1 and u_2 represent the utility for player 1 and 2 respectively:

$$u_1(s) > u_1(\hat{s}) \quad \text{and} \quad u_2(s) < u_2(\hat{s}) \tag{6}$$

A player's gain (or loss) of utility is exactly balanced by the losses (or gains) of the utility of the other player(s) [56]. In other words if a player is increasing his payoff by applying a specific strategy, the same strategy will lead to a reduction in the other players payoff. An interesting class of strictly competitive games is represented by the "zero-sum games" in which the payoffs of the players add up to zero. In a 2 players zero-sum game the following equation is valid:

$$u_1(s_1, s_2) + u_2(s_1, s_2) = 0 \quad \forall\,(s_1, s_2) \tag{7}$$

In other words the payoff that is gained by the first player is exactly the lost in the payoff of the second player [57]. This class of games can be solved by using the Nash equilibrium concept which can be obtained by solving a linear programming problem. In general, assuming that each player (government of attacker) chooses his (defence or attack) strategy according to a rational choice model, given his belief about the other players' strategy and supposing that every player's belief about the other players' actions is correct, a Nash equilibrium can be defined as follows:

Definition 3. *A Nash equilibrium is a strategy s^* with the property that no player i can do better by choosing a strategy different from s_i^*, given that every other player j adheres to s_j^* [58].*

An alternative concept is based on the so called Min-Max theorem which is closely related to linear programming duality [59]. The Min-Max theorem [60] states that in zero-sum games, there always exists a solution of the game.

As emphasized in all the game theory books zero-sum games are easier to be solved than the non zero-sum games and for a 2-players non-repeated zero-sum game, the different solution approaches (Nash equilibrium or the Min-Max theorem) all generate the same solution [57].

In our MISTRAL game, depending on the parameters used inside the model (that are b, B, h_i, f_i, A_{ij}, d_{ij}, β_i, v_i) the resulting utilities for the attacker and the defender might lead to a non zero-sum game. In order to simplify the solution of the MISTRAL game is thus preferable to transform the game into a zero-sum game (see Section 5.1) and then a solution can be obtained by applying the steps depicted in the solution approach which is shown in Figure 3. The final step of the solution approach is referred to as the outcome of the game which is found in compliance with the Definition 1, for a simultaneous-move MISTRAL game, and with the Definition 2, for a sequential-move MISTRAL game. Several applications of the aforementioned solution approach are reported in Sections 5.1, 5.2 and 5.3.

5.1. Transformation into a zero-sum game

In this section the process to transform a non-zero sum MISTRAL game into a zero sum game is explained by means of a practical example. Suppose that four possible defence strategies (denoted by letters d_1, d_2, d_3 and d_4) can be adopted by the government. In addition the same four identical strategies (i.e. having the same level of intensity $d_{ij} = A_{ij}\ \forall\, i, j$) are also available for the attacker (denoted by letters A_1, A_2, A_3 and A_4). Both attack and defence strategies at the inter-modal and intra-modal dimension are represented in Table III.

Based on these attack and defence strategies a MISTRAL game is played once in a simultaneous manner. Combining together the aforementioned attack and defence strategies and by using the MISTRAL parameters defined in Section 4 (that are, b, B, h_i, f_i, β_i, v_i), it is possible to compute the government's and the attacker's payoffs. Since the game is not played sequentially, the payoffs associated to each couple of attacker's and defender's strategies are summarized in a *normal form* by using a payoff matrix as a convenient representation of the MISTRAL game. In Table IV four rows correspond to the four possible strategies of the government, the four columns correspond to the four possible strategies of the attacker. The numbers in each cell represent the players' payoffs associated to the strategies to which the cell corresponds, with the government's payoff listed first.

As it can be observed from the payoff matrix in Table IV the sum of the government's and the attacker's payoffs is not equal to zero for all the strategies pairs. For this reason a transformation of the MISTRAL game into a zero-sum game is needed. The advantage of the transformation is that a zero-sum game always presents an equilibrium.

Using a transformation described in Belavkin [61] it is possible to transform a non zero-sum game into a zero-sum game, so that an equilibrium always exists and its value is equal to the value of the original game. The transformation

is equivalent to the introduction of a passive player whose pure strategy has already been chosen and its associated payoff depends on the strategies adopted by the active players. This transformation is justified by the law of conservation of utility in a game.

The space of the outcomes of that game is $\Omega = \Omega_1 \times \cdots \times \Omega_m$, where Ω_i is the set of pure strategies of player i, and $u_i : \Omega \to \mathbb{R}$ are the utility functions of player i. In a non zero-sum game the following property holds:

$$u_1 + \cdots + u_m \neq 0 \tag{8}$$

By using the bijection $T : U \to \tilde{U}$ where $T(u) = u + u_0$ and $u_0 = -\frac{1}{m}\sum_{i=1}^{m} u_i$ it is possible to transform the players' utility functions in order to generate a zero-sum game. It is easy to demonstrate that the transformed utility functions achieve a zero-sum game:

$$\tilde{u}_1 + \cdots + \tilde{u}_m = \sum_{i=1}^{m}(u_i + u_0) = \sum_{i=1}^{m} u_i + m \cdot u_0 = \sum_{i=1}^{m} u_i - \sum_{i=1}^{m} u_i = 0 \tag{9}$$

In the $\mathcal{MISTRAL}$ model, a possible interpretation of the passive player is represented by society which cannot immediately decide on which security countermeasure to adopt in order to protect an infrastructure, even though it suffers the consequences of a possible attack. The payoff of the passive player is computed by using the following formula:

$$2 \cdot u_0(A, d) = -[u(A, d) + U(A, d)] \tag{10}$$

where the subscript 0 refers to the passive player, whereas $u(A, d)$ and $U(A, d)$ represent the payoffs of the government and of the attacker respectively. The new payoff matrix after the transformation of the original $\mathcal{MISTRAL}$ game into a zero-sum game is represented in Table V in which the passive player and its associate payoffs are omitted to preserve the form of the original payoff matrix.

In Figure 4(a) the original payoffs (for the non-zero $\mathcal{MISTRAL}$ game), associated to each couple of attack and defence strategies, are plotted, whereas in Figure 4(b) the new payoffs associated to the government-attacker, after having transformed the game into a zero-sum $\mathcal{MISTRAL}$ game, are represented. By assessing Figures 4(a) and 4(b) it can be observed that the new payoffs have been rescaled in comparison with the original ones, but their symmetry is preserved, respecting thus the conservation law of utility and equilibria in a non zero-sum game.

5.2. Unlimited attacker's and government's strategies

In this section we assume that the attack or defence levels can assume only three integer values within the range $[1, 3]$ and that no constraint limits the number of available attack and defence strategies. Under these reasonable but

sometimes not completely realistic [2] assumptions and considering the transportation system described in Figure 2, both the government and the attacker have at their disposal a set containing 81 (3^4 that is 3 attack or defence levels that can be associated to each of the 4 available routes) different (defence or attack) strategies. These strategies are obtained by assigning three values for the attack or defence levels to each transportation mode i and route j contained in the transportation system. We assume that both the government and the attacker can freely select their own strategy from the 81 available moves. We conducted an experiment in two different stages. In the first phase we supposed that the $\mathcal{MISTRAL}$ game is played once following a simultaneous-move. In the second phase we assumed that the $\mathcal{MISTRAL}$ game is played once according to a sequential-move game in which the government is the first mover.

In the first case, when both players play at the same time, neither the government nor the defender know in advance the strategy that will be selected by the other player. Following the solution approach summarized in Figure 3 we firstly compute the government's and the attacker's payoffs using Formulae (4) and (5). Then the game is transformed into a zero-sum game using the technique explained in Section 5.1. The normal form of the $\mathcal{MISTRAL}$ game is obtained by generating a payoff matrix which presents 81 rows and columns. The strategies' pair $(A_{81}; d_{81})$ represents the equilibrium of the $\mathcal{MISTRAL}$ game respecting the conditions outlined in Definition 1.

In general in a strategic game, the best strategy for any given player depends on the other players' strategies. So when choosing a strategy a player must have in mind the strategies that the other players will choose. In other words, a player must form a belief about the other players' strategy. In our example, knowing that the government can adopt whatever strategy to prevent an attack, the attacker will try to maximize his utility by setting the attack levels at their highest values. From the opposite perspective, predicting the attacker's behaviour, the government will use an appropriate defence strategy in order to secure the infrastructure which is exposed to the highest threats on all its transportation modes. Therefore the equilibrium consists for the government in an imitation of the attacker's strategy, by adopting the highest levels of defence countermeasures for both the intra-modal and inter-modal levels. This is a rather obvious and logical result. Before elaborating on this outcome further, the $\mathcal{MISTRAL}$ game has been played in a sequential-mode in the second stage of our experiment, where the government is the first mover and then, depending on the adopted defensive strategy, the attacker decides the type of attack to be carried out. In this case, following the solution approach depicted in Figure 3, after having reduced the game into a zero-sum game, an extensive form of

[2] In fact due to a fixed budget at the government's (attacker's) disposal the number of available defence (or/and attack) strategies might be limited. Moreover for technological reasons it might be practically impossible to set a certain level of protection (or attack) for a specific route within a given transportation mode (e.g. for a ground patrol it is practically impossible to secure a pipeline located in a remote area without road infrastructures).

the game, by adopting a tree representation (as the one used in Figure 7), is used to have a better representation of the whole game. Then the $\mathcal{MISTRAL}$ game is solved using the backward induction method [57]. Also in this case, the equilibrium is represented by the couple $(A_{81}; d_{81})$. In fact the government, which plays first, chooses his best strategy anticipating the move of the attacker, in order to limit his own dis-utility in case of attack. For this reason, without any restriction posed, e.g. an existing security budget, the government sets the defence levels at their maximum values. The attacker, which acts only after the government's strategy has been already adopted, chooses the attack for which $d_{ij} = 3 \ \forall i, j$ in order to maximize his utility. Even though the government investments in security assume the highest values for the inter-modal as well as the intra-modal dimension, from the attacker's perspective, strategy A_{81} remains the best alternative, given the current parameters of the $\mathcal{MISTRAL}$ model. In case of a different attack strategy, the investments done for the destruction of the supply chain will lead to lower attacker's returns.

This result might be due to the parameters used inside this specific illustrative example. In particular when the unit cost for attack is higher and the values associated to the losses are lower, the non-attack strategy or an attack directed only on a single intra-modal (or inter-modal) level might be a valid alternative to maximize the attacker's utility.

The solution of the $\mathcal{MISTRAL}$ game in both cases (simultaneous-move and sequential-move) implies for the government an imitation of the opponent's strategy in order to prevent the attacker's actions and limit the consequences of a possible attack. This result is in line with reality in which the defender always attempts to anticipate or respond to the attacker's actions by copying its moves [62]. In other words, referring once again to the "terror alert level" scale, the government adopts e.g. the maximum level of alert and the associated security countermeasures when a severe risk of terrorist attacks is expected (red code alarm). Therefore if the government suspects (e.g. by using the reports of intelligence services) that an attack is possible on a specific route within a particular transportation mode, it will react with proper security countermeasures that compensate the intensity level of the expected attack.

This also explains why authorities generally work with different defence levels: it would be impossible to hold the highest alert for a long time, or it would be unpractical to spend huge budgets to secure all routes and transportation modes. Therefore it is more realistic and interesting to investigate the government's (and/or attackers') behaviour in a $\mathcal{MISTRAL}$ game with restrictions as done in the next section.

5.3. Limited attacker's and government's strategies

In many practical situations limited budgets are available for terrorists (or for institutions) to attack (or to secure) chemical transportation infrastructures. Moreover the presence of other constraints, such as the impossibility to apply a specific attack or security measure to a particular route or transportation

mode, due to technical aspects, might limit the usage of specific defence or attack strategies.

As explained in the previous section, combining together three different values associated to the levels of attack or defence (A_{ij} or d_{ij}) for each transportation mode i which contains route j, it is possible to generate a set of 81 attack and defence strategies. Differently from the previous section, it might be realistic to assume that not all these strategies are at the government's (or the attacker's) disposal at the same time. Moreover, in order to simulate a realistic scenario, without loss of generality, we assume that only four attack or defence strategies are available for the attacker and the defender at each non-repeated $\mathcal{MISTRAL}$ game.

Based on these assumptions we generated all the strategic games that can be obtained by combining together 4 attack and 4 defence strategies per time. In so doing we generated the following number of $\mathcal{MISTRAL}$ games:

$$\binom{A}{4} \cdot \binom{d}{4} = \binom{81}{4} \cdot \binom{81}{4} = \left[\frac{81\,!}{(4\,!) \cdot (81-4)\,!}\right]^2 = 2.76803 \times 10^{12} \qquad (11)$$

As done in the previous section, our experiments have been carried out in two different stages: in the first phase all the resulting $\mathcal{MISTRAL}$ games have been solved on the basis of the simultaneous-mode and then in the second phase of the test the $\mathcal{MISTRAL}$ games have been solved according to the sequential-mode. A computational time equals to 150 hours has been required in total for both the phases of the experiment, using a machine with an Intel core i7-2760QM 2.40GHz processor with 4GB RAM.

In the first stage of the experiment, in 99% of the cases the $\mathcal{MISTRAL}$ games present a saddle point and in 2.25% of the cases the equilibrium consists in an imitation of the opponent's strategy both at the inter-modal and intra-modal dimension. This result is explicable by the fact that in many games the government simply does not have at his disposal an appropriate defensive strategy that can balance the attacker's efforts. In many cases the equilibrium of the game implies for both the government and the attacker the adoption of the available strategies which yield the maximum relative utility.

For a better understanding, an illustrative solution, for the non-repeated $\mathcal{MISTRAL}$ game played in a simultaneous-mode, is reported hereafter. The list of the 4 defensive strategies that the government can use is reported in Figure 5, whereas the attack strategies are shown in Figure 6.

Using the available defence and attack strategies the payoff matrix is built and the game is transformed into a zero-sum game. Therefore a new payoff matrix is obtained (see Table VII).

The matrix in Table VII presents a saddle point and the Min-Max theorem can be applied in order to determine the outcome of the $\mathcal{MISTRAL}$ game which is $(A_1; d_4)$ with an associated payoff equals to 1219 for the attacker and -1219 for the defender.

In the second phase of our experiment we supposed that a limited number of four (attack and defence) strategies are available for each game played once

in a sequential-move where the government is the first player.

Considering all the combinations of 2.76803×10^{12} $\mathcal{MISTRAL}$ games, in 2.87% of the cases the equilibrium consists for the government in an imitation of the opponent's strategy. Considering that the $\mathcal{MISTRAL}$ game is played in a sequential manner, the imitation of the terrorist's actions consists in anticipating the strategy that will be adopted by the attacker. In practice the government attempts to prevent and mitigate the consequences of an attack by adopting appropriate security countermeasures which are addressed at counterbalancing the level of the attacks. From the attacker's perspective, in a sequential game with a limited number of available strategies, an increase in the defensive investments can lead the attacker to either increase his level of efforts (to help compensate for the reduced probability of damages after an attack), or decrease his level of efforts (because attacking has become less profitable). In a symmetrical way this aspect can either reduce or increase the effectiveness of the investments in security from intentional attacks, and can therefore affect the relative desirability of investing to protect infrastructures.

The following example might help to understand the steps which are needed to find the equilibrium for a sequential $\mathcal{MISTRAL}$ game where the government is the first player. We suppose that the same strategies as reported in Figures 5 and 6 are used. In this case the extensive form of the game is presented in Figure 7. The government's and the attacker's payoffs are reported at the bottom of the tree for each leaf node. Government's payoffs are listed first.

Using the backward induction it is possible to find the outcome of the game. The most credible strategies that the attackers will choose in relation to each strategy adopted by the government at the first stage of the game are highlighted by using dotted lines. In particular independently of the government's strategy, the attacker strategy A_1 is the most credible. In fact, for this specific game, A_1 represents the strategy that the attacker will chose in order to maximize its utility. That being so, the government at stage 0 will rationally select strategy d_4 in order to minimize his dis-utility and thus the consequences of the attack. The outcome of the game, according to Definition 2 for a sequential $\mathcal{MISTRAL}$ game, is therefore (A_1, d_4) which is highlighted with red thick lines in Figure 7.

6. Discussion and conclusions

In this paper a model which can guarantee the security of a multi-modal transportation system facing adaptive adversaries has been presented. The model, named $\mathcal{MISTRAL}$, can be used by public and private organizations in order to establish the appropriate allocation of security countermeasures for each route belonging to a specific transportation mode within a chemical supply chain.

Using theorems and concepts borrowed from game theory the $\mathcal{MISTRAL}$ model can be solved by evaluating and analysing the utilities associated to the two players with different interests that are involved in the strategic game. On one side there is the government (or a public-private institution) who intends to protect a given critical infrastructure by allocating adequate security measures

on both the inter-modal and intra-modal levels, and on the other side there is the attacker whose goal is to destroy a targeted supply chain. A methodological scheme to reduce the game into a zero-sum game and, as a result, find the equilibrium, has been presented and applied to a variety of illustrative examples. Several tests have been performed considering both the cases of sequential-move and simultaneous-move with or without unlimited (defence or attack) strategies.

When the number of defence strategies are limited and the MISTRAL game is played simultaneously, the solution of the model consists in adopting the available strategies which can balance the attacker's efforts. In case of sequential game the government should adopt the available security countermeasures aimed at minimizing the utility of the attacker. The latter, depending on the investments in defensive measures by the government, can either increase the attack efforts to compensate the reduced probability of damages after an attack (whether at least one of the available attack strategies can lead to a positive utility from the point of view of the attacker), or reduce the terror acts since no attack strategy is profitable.

Similarly, when no limitations or constraints on the defensive or attack strategies are applied, the solution of the MISTRAL game, in both simultaneous and sequential cases, consists of an imitation of the opponent's strategy. In other words, by using intelligence services the government should try to anticipate the terrorists' moves and guarantee appropriate security levels, which could at least counterbalance the intensity levels of the attacks and mitigate the consequences of an attack. This concept is applied to specific prevention mechanisms adopted by several nations, such as those based on a "terror alert level" scale.

This empirical result is in line with all the practical government guideline used to react to potential terrorist attacks. For example the UK government defines three levels of response which broadly equate to threat levels as shown below [55]:

- *Normal*: routine protective security measures which are appropriate for low and moderate related threat levels;
- *Heightened*: additional and sustainable protective security measures which are recommended for substantial and severe related threat levels in combination with specific business and geographical vulnerabilities and judgements on acceptable risk, in order to reflect the broad nature of the threat;
- *Exceptional*: maximum protective security measures which are suggested for critical related threats levels, in order to meet specific threats and to minimize vulnerability and risk.

In fact the knowledge of the enemy is the basis for whichever strategic choice. As it is asserted in the oldest book on strategy, the *Art of War* written by the Chinese Sun-Tzu [63]:*... if you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle ...* .

Possible applications of the $\mathcal{MISTRAL}$ model pertain to the anticipation of potential attacks to a targeted chemical supply chain and the limitation of the consequences of these attacks thanks to an appropriate evaluation of terrorist threats. Additionally, the $\mathcal{MISTRAL}$ model can lead to a better definition and allocation of the security countermeasures for both intra-modal and inter-modal levels.

Future research will be aimed at extending the current $\mathcal{MISTRAL}$ model to incorporate the case of repeated games. In so doing, it will be possible to simulate realistic scenarios in which continuous attacks are directed to the same supply chain, e.g. the repeated attacks performed on a specific critical pipeline infrastructure [64]. Moreover, additional real-life constraints can be included in the model such as a limited budged for security (or for the attacks), criticality of the infrastructures constituting the whole supply chain and so forth. Additional information about the characteristics of the transported goods can be included in the model. As a matter of fact, the hazardousness of these materials can influence the consequences of a potential attack.

References

[1] Center for Chemical Process Safety CCPS. *Guidelines for Chemical Transportation Safety, Security, and Risk Management*. John Wiley and Sons, Hoboken, New Jersey, 2008.

[2] G. Levitin, W.C. Yeh, and Y. Dai. Minimizing bypass transportation expenses in linear multistate consecutively-connected systems. *IEEE*, 2014.

[3] E. Erkut and V. Verter. Modeling of transport risk for hazardous materials. *Operations Research*, 46(5):625–642, 1998.

[4] S. Contini, F. Bellezza, M.D. Christou, and C. Kirchsteiger. The use of geographic information systems in major accident risk assessment and management. *Journal of Hazardous Materials*, 78(1-3):223–245, 2000.

[5] B. Fabiano, F. Curro, E. Palazzi, and R. Pastorino. A framework for risk-management and decision-making strategies in dangerous good transportation. *Journal of Hazardous Materials*, 93:1–15, 2002.

[6] E. Erkut, S.A. Tjandra, and V. Verter. Chapter 9 hazardous materials transportation. In Cynthia Barnhart and Gilbert Laporte, editors, *Transportation*, volume 14 of *Handbooks in Operations Research and Management Science*, pages 539–621. Elsevier, 2007.

[7] F. Tena-Chollet, J. Tixier, G. Dusserre, and J.F. Mangin. Development of a spatial risk assessment tool for the transportation of hydrocarbons: Methodology and implementation in a geographical information system. *Environmental Modelling & Software*, 46(0):61 – 74, 2013.

[8] J. Zhang, J. Hodgson, and E. Erkut. Using GIS to assess the risks of hazardous materials transport in networks. *European Journal of Operational Research*, 121 (2):316–329, 2000.

[9] V. Verter and B.Y. Kara. A GIS-based framework for hazardous materials transport risk assessment. *Risk analysis*, 21(6):1109–1120, 2001.

[10] P. Dell'Olmo, M. Gentili, and A. Scozzari. On finding dissimilar pareto-optimal paths. *European Journal of Operational Research*, 162(1):70–82, 2005.

[11] P. Carotenuto, S. Giordani, and S. Ricciardelli. Finding minimum and equitable risk routes for hazmat shipments. *Computers & Operations Research*, 34(5):1304–1327, 2007.

[12] W. Jianxin, W. Tong, M. Yunfei, and T. Jialei. Study on the dangerous chemicals transport vehicles monitoring system based on RFID technique. In Zhenyu Du, editor, *Intelligence Computation and Evolutionary Computation*, volume 180 of *Advances in Intelligent Systems and Computing*, pages 1015–1019. Springer Berlin Heidelberg, 2013.

[13] A. Preda, M. Rönkkö, S. Pickl, and M. Kolehmainen. GIS-based route planning for HAZMAT transportation. In Jiří Hřebíček, Gerald Schimak, Miroslav Kubásek, and Andrea E. Rizzoli, editors, *Environmental Software Systems. Fostering Information Sharing*, volume 413 of *IFIP Advances in Information and Communication Technology*, pages 357–366. Springer Berlin Heidelberg, 2013.

[14] R. Bubbico, S. Di Cave, and B. Mazzarotta. Risk analysis for road and rail transport of hazardous materials: a GIS approach. *Journal of Loss Prevention in the Process Industries*, 17(6):483 – 488, 2004.

[15] B.Y. Kara, E. Erkut, and V. Verter. Accurate calculation of hazardous materials transport risks. *Operations Research Letters*, 31(4):285–292, 2003.

[16] E. Erkut and F. Gzara. Solving the hazmat transport network design problem. *Computers & Operations Research*, 35(7):2234–2247, 2008.

[17] J. Xu, J. Gang, and X. Lei. Hazmats transportation network design model with emergency response under complex fuzzy environment. *Mathematical Problems in Engineering*, 2013:1–22, 2013.

[18] B.Y. Kara and V. Verter. Designing a road network for hazardous materials transportation. *Transportation Science*, 38(2):188–196, 2004.

[19] O. Berman, V. Verter, and B.Y. Kara. Designing emergency response networks for hazardous materials transportation. *Computers & Operations Research*, 34 (5):1374–1388, 2007.

[20] V.M. Bier, N. Haphuriwat, J. Menoyo, R. Zimmerman, and A Culpen. Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Analysis*, 28(3):763–770, 2008.

[21] J. Zhuang and V.M. Bier. Balancing terrorism and natural disasters-defensive strategy with endogenous attack effort. *Operations Research*, 55(5):976–991, 2007.

[22] G. Heal and H. Kunreuther. Modeling interdependent risks. *Risk Analysis*, 27 (3):621–634, 2007.

[23] P. Paruchuri, J.P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus. Efficient algorithms to solve bayesian stackelberg games for security applications. In *Proceedings of the 23rd national conference on articicial intelligence*, volume 3, pages 1559–1562. AAAI Press, 2008.

[24] N. Dighe, Zhuang J., and Bier V.M. Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence. *International Journal of Performability Engineering, special issue on System Survivability and Defense against External Impacts*, 5(1):31–43, 2009.

[25] S.D. Guikema and T. Aven. Assessing risk from intelligent attacks: A perspective on approaches. *Reliability Engineering and System Safety*, 95(5):478–483, 2010.

[26] J. Zhuang, V.M. Bier, and O. Alagoz. Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *European Journal of Operational Research*, 203(2):409–418, 2010.

[27] T. Sandler and K. Siqueira. Games and terrorism. *Simulation & Gaming*, 40(2): 164–192, 2009.

[28] K. Hausken and G. Levitin. Review of systems defense and attack models. *International Journal of Performability Engineering*, 8(4):355, 2012.

[29] N. Azaiez and V.M. Bier. Optimal resource allocation for security in reliability systems. *European Journal of Operational Research*, 181(2):773–786, 2007.

[30] S. Patterson and G. Apostolakis. Identification of critical locations across multiple infrastructures for terrorist actions. *Reliability Engineering & System Safety*, 92 (9):1183–1203, 2007.

[31] G. Levitin and K. Hausken. Protection vs. redundancy in homogeneous parallel systems. *Reliability Engineering & System Safety*, 93(10):1444–1451, 2008.

[32] K. Hausken. Strategic defense and attack for reliability systems. *Reliability Engineering and System Safety*, 93(11):1740–1750, 2008.

[33] D. Liu, X. Wang, and J. Camp. Game-theoretic modeling and analysis of insider threats. *International Journal of Critical Infrastructure Protection*, 1:75–80, 2008.

[34] K. Hausken and G. Levitin. Minmax defense strategy for complex multi-state systems. *Reliability Engineering and System Safety*, 94(2):577–587, 2009.

[35] B. Golany, E.H. Kaplan, A. Marmur, and U.G. Rothblum. Nature plays with dice terrorists do not: allocating resources to counter strategic versus probabilistic risks. *European Journal of Operational Research*, 192(1):198–208, 2009.

[36] G. Reniers. An external domino effects investment approach to improve cross-plant safety within chemical clusters. *Journal of Hazardous Materials*, 117(1-3): 167–174, 2010.

[37] X. Gao, W. Zhong, and S. Mei. Information security investment when hackers disseminate knowledge. *Decision Analysis*, 10(4):352–368, 2013.

[38] A. Roy and P. Jomon Aliyas. Terrorism deterrence in a two country framework: strategic interactions between r&d, defense and pre-emption. *Annals of Operations Research*, 211(1):399–432, 2013.

[39] K. Hausken and J. Zhuang. The impact of disaster on the strategic interaction between company and government. *European Journal of Operational Research*, 225(2):363 – 376, 2013.

[40] A. Samuel and S.D. Guikema. Resource allocation for homeland defense: Dealing with the team effect. *Decision Analysis*, 9(3):238–252, 2012.

[41] J. Merrick and G.S. Parnell. A comparative analysis of pra and intelligent adversary methods for counterterrorism risk management. *Risk Analysis*, 31(9): 1488–1510, 2011.

[42] L. Zamparini. Transport security in EU and US: Competing or complementary visions? In *Nectar workshop on transport security*, Lecce, Italy, 5-6 Feb 2010.

[43] L.A. Cox. Game theory and risk analysis. *Risk Analysis*, 29(8):1062–1068, 2009.

[44] R. McDermott and P.G. Zimbardo. The psychological consequences of terrorist alerts. *Psychology of terrorism*, pages 357–370, 2007.

[45] S. Skaperdas. Contest success functions. *Economic Theory*, 7:283–290, 1996.

[46] V.M. Bier, A. Nagaraj, and V. Abhichandani. Protection of simple series and parallel systems with components of different values. *Reliability Engineering and System Safety*, 87(3):315–323, 2005.

[47] W. Enders and E. Olson. Measuring the economic costs of terrorism. *The Oxford Handbook of the Economics of Peace and Conflict*, page 874, 2012.

[48] G.A. Karolyi and R. Martell. Terrorism and the stock market. *International Review of Applied Financial Issues and Economics*, (2):285–314, 2010.

[49] T. Sandler and W. Enders. Economic consequences of terrorism in developed and developing countries. *Terrorism, economic development, and political openness*, 17, 2008.

[50] M.J. Osborne. *An Introduction to Game Theory*. Oxford University Press, USA, 2003.

[51] X. Gao, W. Zhong, and S. Mei. A game-theory approach to configuration of detection software with decision errors. *Reliability Engineering & System Safety*, 119(0):35–43, 2013.

[52] X. Shan and J. Zhuang. Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender-attacker game. *European Journal of Operational Research*, 228(1):262–272, 2013.

[53] N.O. Bakir. A stackelberg game model for resource allocation in cargo container security. *Annals of Operations Research*, 187(1):5–22, 2011.

[54] Homeland Security Advisory Council HSAC. Homeland security advisory system, task force report and recommendaations. Technical report, U.S. Department of Homeland Security, September 2009.

[55] UK Cabinet Office. Threat levels: The system to assess the threat from international terrorism. Guidance Policy: Protecting the UK against terrorism, National security and intelligence, St Clements House, 2-16 Colegate, Norwich, UK, July 2006.

[56] A.M. Colman. *Game Theory and its Applications in the Social and Biological Sciences*. International Series in Social Psychology. Butterworth-Heinemann Ltd, 1995.

[57] J.N. Webb. *Game Theory. Decision, Interaction and Evolution*. Springer Undergraduate Mathematics Series. Springer, 2007.

[58] T.E.S. Raghavan. Zero-sum two person games. In Robert A. Meyers, editor, *Computational Complexity*, pages 3372–3395. Springer New York, 2012.

[59] K. Binmore. *Playing for Real: A Text on Game Theory*. Oxford University Press, USA, 2007.

[60] J. Von Neumann and O. Morgenstern. *Theory of games and economic behavior*. Princeton University Press, Princeton, NJ, 1944.

[61] R.V. Belavkin. Conservation law of utility and equilibria in non-zero sum games.

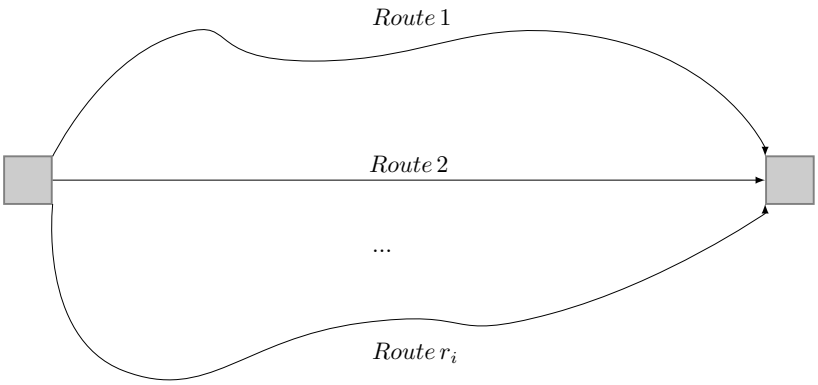
CoRR, abs/1010.2439, 2010.

[62] M.R. Ronczkowski. *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis and Investigations*. CRC Press, Taylor & Francis Group, 2006.

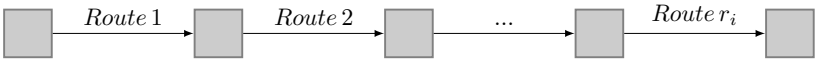
[63] Sun-Tzu. *The Art of War*. Simon & Brown, 2014.

[64] L. Talarico, K. Sörensen, G.L.L. Reniers, and J. Springael. *Securing Transportation Systems*, chapter Pipeline Security. Springer Science and Business Media, LLC, New York, in press 2015.

Figures and Tables



(a) Parallel structure



(b) Serial structure

Figure 1: Parallel (a) and Serial (b) transportation structures

Table I: Main assumptions in the $\mathcal{MISTRAL}$ model

#	**Assumption**
1	$\beta_1 > \beta_2 > \beta_3 > \beta_4$
2	$\partial P_{ij}/\partial d_{ij} \leq 0$, $\partial P_{ij}/\partial A_{ij} \geq 0$ and $P_{ij}(0, d_{ij}) = 0 \; \forall \, d_{ij}$
3	*Parallel structure* for $i = 2, 4$ and *serial structure* for $i = 1, 3$
4	$f_2 < f_4 < f_1 < f_3$ and $h_1 < h_4 < h_2 < h_3$

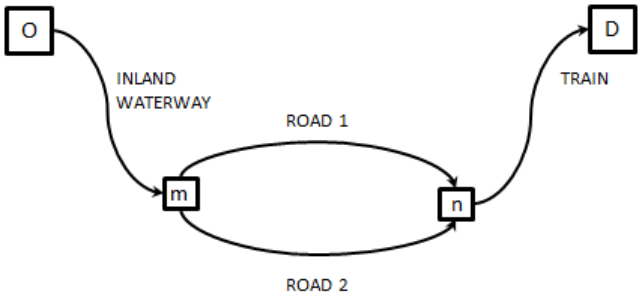


Figure 2: Example of a transportation system for chemical materials

i	f_i	h_i
1	200	5
2	100	15
3	300	25

Table II: Values associated to financial and human losses

(a) Strategies A_1 and d_1

i/j	1	2
1	3	
2	1	1
3	1	

(b) Strategies A_2 and d_2

i/j	1	2
1	2	
2	2	2
3	2	

(c) Strategies A_3 and d_3

i/j	1	2
1	3	
2	2	1
3	2	

(d) Strategies A_4 and d_4

i/j	1	2
1	3	
2	2	2
3	3	

Table III: List of attack and defence strategies available for the attacker and the government respectively

	A_1	A_2	A_3	A_4
d_1	(2722; 6218)	(1724; 7196)	(1603; 7317)	(1321; 7579)
d_2	(3801; 4939)	(2522; 6198)	(2407; 6313)	(1986; 6714)
d_3	(3916; 4824)	(2643; 6077)	(2522; 6198)	(2100; 6600)
d_4	(4250; 4290)	(2934; 5586)	(2813; 5707)	(2322; 6178)

Table IV: Payoff Matrix

	A_1	A_2	A_3	A_4
d_1	(-4470;-1748)	(-4370;-569)	(-4370;-454)	(-4270;-20)
d_2	(-4460;-2736)	(-4360;-1838)	(-4360;-1717)	(-4260;-1326)
d_3	(-4460;-2857)	(-4360;-1953)	(-4360;-1838)	(-4260;-1447)
d_4	(-4450;-3129)	(-4350;-2364)	(-4350;-2250)	(-4250;-1928)

Table V: Payoff matrix after the transportation into a zero-sum $\mathcal{MISTRAL}$ game

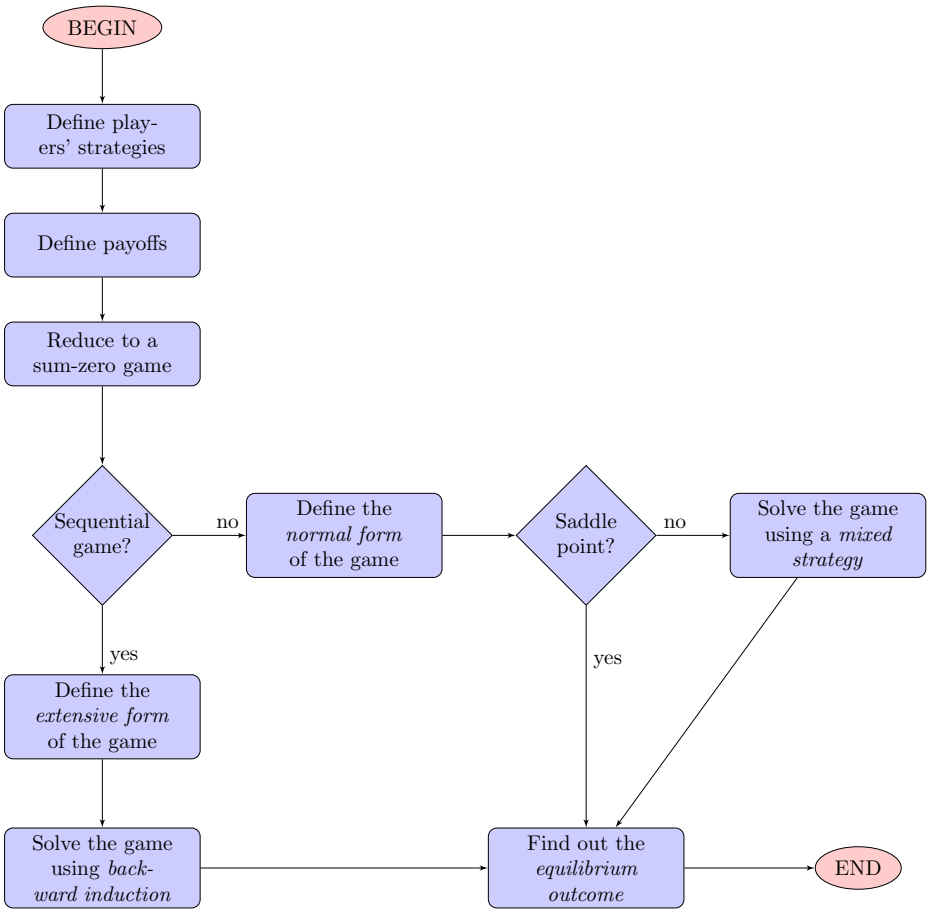
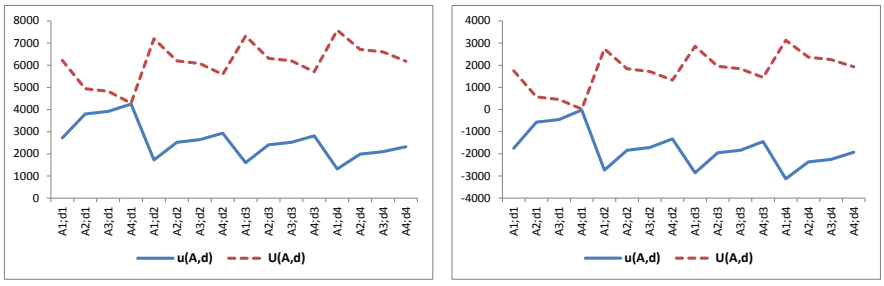


Figure 3: Flow chart used to solve the strategic $\mathcal{MISTRAL}$ game



(a) Original payoffs (b) Transformed payoffs

Figure 4: Government's and attacker's payoffs before (a) and after (b) the transformation into a zero-sum game

(a) Attack strategy A_{81}

i/j	1	2
1	3	
2	3	3
3	3	

(b) defence strategy d_{81}

i/j	1	2
1	3	
2	3	3
3	3	

Table VI: Equilibrium of the $\mathcal{MISTRAL}$ game played once with a simultaneous-move

i/j	1	2
1	1	
2	2	1
3	2	

(a) defence strategy d_1

i/j	1	2
1	3	
2	3	2
3	1	

(b) defence strategy d_2

i/j	1	2
1	2	
2	1	3
3	2	

(c) defence strategy d_3

i/j	1	2
1	3	
2	3	1
3	2	

(d) defence strategy d_4

Figure 5: Available strategies for the government

i/j	1	2
1	3	
2	1	2
3	3	

(a) Attack strategy A_1

i/j	1	2
1	2	
2	2	1
3	1	

(b) Attack strategy A_2

i/j	1	2
1	1	
2	2	1
3	3	

(c) Attack strategy A_3

i/j	1	2
1	2	
2	3	1
3	2	

(d) Attack strategy A_4

Figure 6: Available strategies for the attacker

	A_1	A_2	A_3	A_4
d_1	(-1576;1576)	(-343;343)	(-1439;1439)	(-1372;1372)
d_2	(-1591;1591)	(-582;582)	(-1335;1335)	(-1382;1382)
d_3	(-1452;1452)	(103;-103)	(-974;974)	(-824;824)
d_4	**(-1219;1219)**	(6;-6)	(-1081;1081)	(-1041;1041)

Table VII: Payoff matrix for the zero-sum $\mathcal{MISTRAL}$ game in a simultaneous-move. The equilibrium of the game is reported in bold

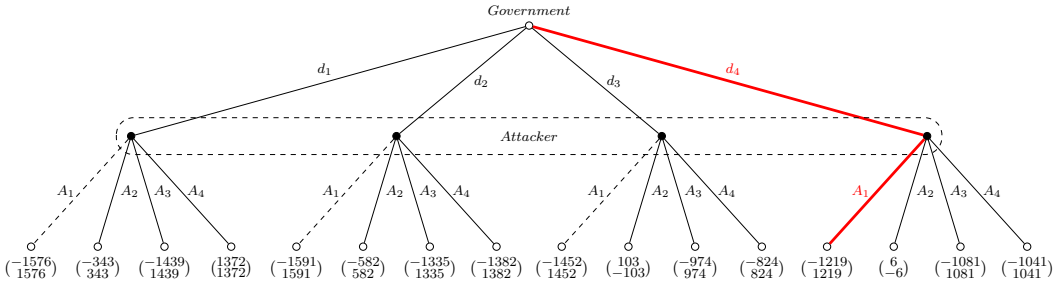


Figure 7: Extensive form of the $\mathcal{MISTRAL}$ game